العنوان: الأضرار الاقتصادية للجرائم المعلوماتية وإستراتيجية مكافحتها عربياً ودولياً

المصدر: المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية- ICACC - كلية علوم الحاسب والمعلومات - جامعة الإمام محمد بن سعود الإسلامية - السعودية

المؤلف الرئيسي: سرحان، القروي بشير

محكمة: نعم

التاريخ الميلادي: 2015

مكان انعقاد المؤتمر: المملكة العربية السعودية. الرياض

رقم المؤتمر: 1

الهيئة المسؤولة: جامعة الإمام محمد بن سعود الإسلامية. كلية علوم الحاسب والمعلومات

الشهر: نوفمبر

الصفحات: 66 - 74

رقم MD: 690591

نوع المحتوى: بحوث المؤتمرات

قواعد المعلومات: HumanIndex

مواضيع: الجريمة المعلوماتية

رابط: http://search.mandumah.com/Record/690591

الأضرار الاقتصادية للجرائم المعلوماتية واستراتيجية مكافحتها عربيا ودوليا

د. القروي بشير سرحان
أستاذ محاضر بكلية الحقوق والعلوم السياسية
جامعة الجيلالي بونعامة خميس مليانة
الجزائر
elgaroui@hotmail.com

الملخص- لقد اختصرت التكنولوجيا المسافات واختزلت الزمن، حتى أصبح العالم قرية واحدة يتصل فيها من هو يقطن في القطب الشمالي بشخص آخر في القطب الجنوبي في ثواني معدودة، إن ما توفره تكنولوجيا المعلومات والاتصالات في عالمنا اليوم يفوق التصورات، ولكنه بالمقابل جلب معه تهديدات ومخاطر كثيرة، بدءا بالخطر الثقافي والاجتماعي وصولا إلى المخاطر الاقتصادية التي تحدثها ما أصبح يطلق عليه الآن بالجريمة المعلوماتية، والتي أصبحت لا تهدد الفرد فقط بل امتد تهديدها ليصل حتى الدول، ومنه لا أحد بمنأى منها، ولأجل هذا تزايد الاهتمام بدراسة الجريمة المعلوماتية وأثرها على الفرد والدول، وهذا ما سنحاول التطرق إليه من خلال هذه الورقة البحثية.

الكلمات المفتاحية- الجريمة المعلوماتية، الجريمة الاقتصادية، الفيروسات، الهجمات الإلكترونية، الحاسوب، المعلومات، الإرهاب الإلكتروني، استراتيجية مكافحة الجريمة المعلوماتية.

مقدمة:

لقد كان لإفرازات العولمة آثار إيجابية وأخرى سلبية، ولعل من أخطر الآثار السلبية للعولمة هي الجرائم الإلكترونية التي أصبحت لا تهدد الأفراد فقط، وإنما امتد تهديدها للمجتمعات والدول ومنه أصبحت الحكومات تأخذ هذه التهديدات محل الجد، فإذا كانت الدول في الماضي تجهز جيوشها للتصدي لأي غزو خارجي أو تهديد لأمنها وسلامتها، فهي الآن مجبرة على تجهيز جيشها الإلكتروني للتصدي للهجمات التي تشن عليها.

ولقد أثبت الواقع الذي تعيشه الدول في العديد من المرات خطورة الهجمات التي تشن ضدها، فعلى سبيل المثال لا الحصر تم تعطيل دولة بكاملها مثل دولة "ليتوانيا" بفعل الهجمات أو الحرب الإلكترونية التي شنت ضدها من طرف القراصنة الروس، ولن نطيل كثيرا في سرد أحداث الهجمات الإلكترونية على الدول والأجهزة الحساسة في الدولة، أو حتى بعض الشركات الكبرى فمثلا شركة بحجم شركة "أرامكو السعودية" تعرضت لأعنف الهجمات الإلكترونية قصد تعطيل صناعة النفط، وآخر الأخبار للهجمات الإلكترونية هي ما تعرضت به شركة عملاقة مثل شركة "سوني SONY" من تعطيل وتخريب لنظام المعلومات لديها والتي سببت لها خسائر مالية معتبرة.

ويعود تاريخ أول جريمة إلكترونية سنة ١٩٥٨، ومنه شرع في رصد ونشر ما تتوافر بشأنه التقارير من حالات إساءة استخدام الحاسوب في أمريكا، وحيث صنفت آنذاك ضمن جرائم العبث والتخريب الموجه إلى الحاسوب، سرقة المعلومات أو الممتلكات، لاحتيال أو الغش المالي، والاستخدام غير المصرح به لخدمات الحاسوب، وكانت الأنشطة الإجرامية المتصلة بالحاسوب تتعلق بالجانب غير الأخلاقي لاستعمال الحاسوب، ولم تكن تستند إلى أي أساس قانوني لتجريمها والعقاب عليها[١].

ولقد جلب عقد السبعينات بذور ملامح ظاهرة جرائم الحاسوب، فإن عقدي الثمانينات والتسعينات وحاضرنا جلبا مفهوم وماهية هذه الجرائم، وبالمقابل الشعور بعظم هذه الظاهرة وضرورة التصدي لها من خلال توفير الوسائل القانونية والفنية الفاعلة لمعالجتها، فقد قدم معهد "ستانفورد" استبيان للتحضير لمناقشة مشروع قانون الجريمة الاقتصادية[٢]، أما معهد الإجرام وقانون العقوبات الاقتصادي في ألمانيا الاتحادية قام بتقديم دراسة تضمنت وصفا لـ٣١ جريمة ارتكبت بواسطة الحاسوب[٣].

وبعدها توالت الدراسات التي سجلت رصد العديد من جرائم الحاسوب، وبهذا بدأت بعض الدول تواجه النمط الجديد من الحروب الإلكترونية والإرهاب الإلكتروني كما تم على الصعيد الدولي إبرام العديد من الاتفاقيات الدولية في محاولة لترسيخ وجوب التعاون الدولي لمواجهة جرائم الكمبيوتر[٤].

وقبل الخوض في صلب الموضوع، حري بنا التطرق إلى تعريف الجريمة الإلكترونية، وفي هذا المجال نشير إلى أنه لا يوجد تعريف جامع للجريمة الإلكترونية، وكما يقول فإن دير هلست: "هناك غياب لتعريف عام وإطار نظري متسق في هذا الحقل... وفي أغلب الأحيان تستخدم مصطلحات الافتراضية، والحاسوب، والإلكترونية، والرقمية، وكلها تعكس فجوات مهمة في التعريف"(٥).

ولكنه بالمقابل يمكننا أن نذكر في هذا المجال تعريفين، وحدا فنيا والآخر تعريف قانوني للجريمة الإلكترونية، فبالنسبة للتعريف الفني للجريمة الإلكترونية هي: "عبارة عن نشاط إجرامي تستخدم فيه تقنية الحاسب الآلي بطريقة مباشرة كوسيلة أو هدف لتنفيذ الفعل الإجرامي"(٦).

وأما بالنسبة للتعريف القانوني فتعرف بأنها: "مجموعة من الأفعال والأنشطة المعاقب عليها والتي تربط بين الفعل الإجرامي والثورة التكنولوجية"، وتعرف أيضا: "نشاط جنائي يمثل اعتداء على برامج الحاسب الآلي"(٧).

وفي هذا السياق وبعد أن أعطينا تعريفا مختصرا للجريمة الإلكترونية، سنحاول التطرق إلى الآثار الوخيمة التي تسببها الهجمات الإلكترونية من الناحية الاقتصادية، والاستراتيجية الدولية، والعربية لمواجهتها.

ومنه سنتطرق إلى هذا الموضوع من خلال طرح الإشكالية التالية:

ما هي الأضرار الآنية والمستقبلية التي تحدثها الهجمات الإلكترونية والتي تستهدف البيانات والمعلومات على اقتصاد الدولة والشركات الخاصة والعامة التابعة لها؟

وما هي الاستراتيجية المتبناة دوليا وعربيا لمواجهتها؟

وهل هذه الاستراتيجيات هي كفيلة لردع ومكافحة الجرائم المعلوماتية؟

وسعيا منا على الإجابة على هذه الإشكالية ارتأينا تقسيم موضوعنا إلى الخطة التالية:

المحور الأول: أثر الهجمات الإلكترونية على اقتصاديات الدول.

المحور الثاني: استراتيجية مكافحة الجريمة المعلوماتية على الصعيد الدولي.

المحور الثالث: استراتيجية مكافحة الجريمة المعلوماتية على الصعيد العربي.

المحور الأول: أثر الهجمات الإلكترونية على اقتصاديات الدول:

لقد أضحى العالم اليوم رهين كبسة زر سواء للتشغيل أو توقيف التشغيل، في عالم تزايد فيه استخدام الحواسيب حتى طال كل شيء، فلا يخلو مجال إلا ووجدنا فيه الحواسيب حتى الدول أصبحت تعتمد في تسييرها على الحاسب الآلي، وهذا ما يسمى بالحكومة الإلكترونية، والتي أصبحت إحدى وسائل تحقيق الحكم الراشد، ولكنه في المقابل بقدر تزايد استعمال الحاسب الآلي بقدر ما تزايدت التهديدات وأصبحت المخاطر تتهدد الحكومات بشكل عام والمنظمات والشركات بشكل خاص، بل وحتى الأفراد لم يصبحوا بمأمن من التهديدات والمخاطر التي تأتي عبر الحواسيب الآلية، حيث ظهر نوع جديد من الجرائم يعرف بالجريمة الإلكترونية، وقد انتشرت هذه الجرائم بشكل مخيف جدا، فضحايا الجرائم الإلكترونية وعلى تنوعهم يتعرضون لتعطيل وتدمير قواعد البيانات والمعلومات الخاصة بهم ويتعرضون إلى سرقة أموالهم بالإضافة إلى التهديد والابتزاز، وكل هذه الجرائم تؤثر بشكل سلبي على الاقتصاد.

ونشير أن معدل نسبة الجرائم الإلكترونية في العالم يصل إلى ٥٧،٦%، بحيث تكلف هذه الجرائم الاقتصاد العالمي ما يقارب ١٢،٩٥٠ مليار دولار سنويا، كما كشفت السلطات الأمريكية سنة ٢٠٠٩ أن عمليات قرصنة وسرقة طالت ١٣٠ مليون بطاقة ائتمان وبطاقة سحب مصرفية، وقد تم تقدير حجم الخسائر الاقتصادية في أول مؤتمر متخصص لمحاربة الجريمة الإلكترونية، والذي عقد عام ٢٠٠٩ بمدينة "هونغ كونغ" بـ٥٠١ مليار دولار سنويا، حيث تتكبد الشركات الأوروبية خسائر تقدر بتريليون دولار سنويا بينما تتكبد الشركات الأمريكية ٨،٣ مليار دولار سنويا(٨).

وأظهر تقرير نشرته "سيمانتك كوربوريشن" تزايد ملفت للنظر بالنسبة للهجمات الإلكترونية، بحيث قد تم رصد ما يقارب ١٠٠ هجوم في الثانية، وفي دراسة أجرتها شركة نورتن- Norton-، وهي شركة رائدة في تطوير الحلول البرمجية الأمنية، أن ثلثي مستخدمي الإنترنت حول العالم تعرضوا لجريمة إلكترونية على الأقل بحيث أنهم تعرضوا إلى هجمات فيروسية أو تجسيسية أو احتيالية لسرقة بطاقات الائتمان من أجل سرقة الهوية أو البيانات المصرفية والشخصية الحساسة(٩).

وكما أشارت الدراسة أن عملية إصلاح وإزالة ما تسببه الهجمات الإلكترونية من آثار يستغرق في المتوسط ٢٨ يوما، وتكلف هذه العملية في المتوسط ٣٣٤ دولار(١٠).

وتشير بعض التوقعات بأن حجم الخسائر التي تحدثها الجريمة الإلكترونية في دول مجلس التعاون الخليجي ما بين ٥٥٠ مليون و٧٣٥ مليون دولار أمريكي سنويا، وتعتبر كل من المملكة العربية السعودية والإمارات العربية المتحدة من أكثر الدول تعرضا للهجمات الإلكترونية(١١).

وحسب المعطيات التي قدمها خبير اقتصادي، أكد فيه أن نسبة معدل الهجمات في المملكة العربية السعودية تقارب ٤٥،٨% لعام ٢٠٠٩، وبالنسبة لهجمات الحسابات البنكية للأفراد بلغت ٤٠% من نفس السنة، وبالنسبة لاختراق المواقع الإلكترونية فقد بلغ ٦٣%، ورسائل الاحتيال بلغت ٤٣،٧% وفي دراسة أجرتها شركة "تريند مايكرو" وهي شركة مشهورة بمحاربة الفيروسات، أشارت إلى انهيار ٧٠٠ ألف نظام خلال تسعة أشهر في المملكة العربية السعودية(١٢).

إن الجريمة الإلكترونية لا تطال فقط الدول، بل تطال كل مستخدم لحاسب آلي مربوط بشبكة الإنترنت وعليه فيمكن حصر مستويات الجريمة الإلكترونية في ثلاث مستويات وهي ، الفرد الشركات والدول ، وعليه سنحاول التطرق إلي هذه المستويات وتحديد أثر الهجمات الإلكترونية عليها

١. أثر الهجمات الإلكترونية على الفرد:

يعتبر الأفراد الحلقة الضعيفة في نظام المعلومات، وكثيرا ما يتعرضون إلى مختلف أنواع صور الجريمة المعلوماتية، فبعد ما اكتسب التعامل بالأموال في عصر المعلوماتية صفة البيانات الإلكترونية وبالتالي أصبح بمقدور الأفراد إجراء تحويلات ومبادلات مالية من أي مكان في العالم، وبهذا أصبحت هذه البيانات عرضة للسرقة، وتتم سرقة البيانات بانتهاج إحدى الطريقتين وهما:

- الطريقة الأولى: تكمن آلية السرقة في استقطاع بعض السنتيمات(١٣) من الإيداعات الدورية.
- الطريقة الثانية/ وتعرف بطريقة سلامي- salami- وتكمن في تقنية استقطاع مبالغ صغيرة من حسابات مالية ضخمة، وتحويلها آليا عبر الفضاء الإلكتروني- cyber space- إلى حساب الجاني الشخصي ليستخدمها فيما بعد(١٤).

كما يتعرض الأفراد كثيرا إلى عملية احتيال لاستخدام بطاقات الائتمان، فقد تم سرقة مئات الألوف من أرقام بطاقات الائتمان في يوم واحد من خلال شبكة الإنترنيت ومن ثم بيع هذه المعلومات للآخرين وبينت شركة تور قروب- TOWER GROUPE- أن ١١% من المبادلات بواسطة البطاقات الائتمانية عبر شبكة الإنترنيت مزورة، وأن قيمة أعمال التزوير عبر الإنترنيت تصل إلى ٤٣ مليون دولار(١٥).

وقد اكتشفت بعض البنوك تكرار عملية اعتراض حاملي بطاقات الدفع الإلكتروني على عمليات لم يقوموا بإجرائها، وتبين فيما بعد أنها عمليات تم إجراؤها عن طريق شبكة الإنترنيت بواسطة بعض الهواة المتطفلين- hackers- والمخربين- crsckers- حيث تمكنوا من التقاط وتخليق أرقام لبطاقات الدفع الإلكتروني الخاصة ببعض العملاء على الشبكة واستغلالها في الحصول على السلع والخدمات(١٦).

ومن الأمثلة الواقعية لاحتيال بطاقات الائتمان واقعة المتطفل كيفين ميتنك- Kevin mitnick- الذي أسندت له تهمة استخدام وسيلة دخول احتيالية والاحتيال على الكمبيوتر من أجل الحصول على ٢٠،٠٠٠ بطاقة ائتمان من شركة للاتصالات في سان جوس- San Jose- بكاليفورنيا بالولايات المتحدة الأمريكية(١٧).

وعليه، فكثيرة هي الجرائم التي تقع على الأشخاص، وقد حاولنا فقط ذكر الأكثر انتشارا وبخاصة بعد انتشار التجارة الإلكترونية، وما حملته من مخاطر على الفرد، وبالإضافة إلى ما تم ذكره من جرائم معلومات تقع على الأفراد يمكننا أن نشير إلى جرائم أخرى وهي:

- سرقة الهوية الشخصية.
- الابتزاز والتهديد.
- عملية النصب والاحتيال.
- تحويل أو نقل الحساب المصرفي.
- نقل ملكية الأسهم.
- زيادة الفواتير بتحويل فواتير المجرم للضحية(١٨).

وهناك جرائم أخرى تصيب الفرد لا يسع المجال لذكرها كلها، وما يمكن قوله عن الجرائم السالفة الذكر أنها تحدث خسائر مالية لها انعكاسات سلبية على الذمة المالية للفرد بصفة خاصة، بالإضافة إلى التأثيرات السلبية على الاقتصاد بشكل عام.

٢. **أثر الهجمات الإلكترونية على المؤسسات والشركات:** لقد تطور شكل عمل المؤسسات والبنوك بشكل جذري ولافت، وأصبحت تعتمد بشكل يكاد يكون كلي على الحاسب الآلي في تعاملاتها اليومية وفي اتصالاتها مع زبائنها، وبالتالي باتت هذه المؤسسات والشركات عرضة للهجمات الإلكترونية وقد أظهرت دراسة قامت بها الأمم المتحدة حول جرائم الحاسوب والإنترنيت بأن ٢٤-٤٢% من منظمات القطاع العام والخاص على حد السواء، كان ضحية لجرائم تتعلق بالحاسب الآلي والإنترنيت[١٩].

وقد أشارت دراسة جديدة أن جرائم الإنترنيت تكلف الاقتصاد العالمي نحو ٤٤٥ مليار دولار كل عام وأن الأضرار التي لحقت بقطاع الأعمال نتيجة سرقة الملكية الفكرية تتسبب بخسارة الأفراد لحوالي ١٦٠ مليار دولار، ووجدت الدراسة أن أكبر الاقتصاديات في العالم تحملت وطأة هذه الخسائر، حيث بلغ إجمالي خسائر الولايات المتحدة الأمريكية والصين واليابان وألمانيا ٢٠٠ مليار دولار سنويا[٢٠].

وبالنسبة لوقع الهجمات الإلكترونية على الشركات، فقد أعلن مكتب التحقيقات الفيدرالي الأمريكي أن جميع الشركات الكبرى (تقريبا ٥٠٠ شركة) تعرضت لهجوم عبر الإنترنيت، وأن ما أنفقته مؤسسات الأعمال لمكافحة المخربين والفيروسات تجاوز ٣٠٠ مليار دولار في عام ٢٠٠٠(٢١)، كما نشير أن هناك صعوبة في قياس القيمة الاقتصادية للأضرار الناجمة عن الجرائم المعلوماتية بسبب غياب المنهجية المعتمدة لتقدير الأضرار فضلا عن تردد المنشآت والهيئات في الإفصاح عن تعرضها للهجوم في وقت مبكر، ومن جهة أخرى تجنب الشركات المستهدفة للإعلان عن حوادث الهجوم، بحيث يؤدي إلى التقليل من عنصر الإيرادات الضائعة ويجعله في المرتبة الثانية، كما أن الجريمة المعلوماتية تؤثر في أسعار الأسهم، حيث أظهرت دراسة أن الشركات التي تعرضت لاختراق معلوماتي تعاني من هبوط أسهمها في حدود ١%-٥% في اليوم التالي لإعلان الاعتداء مباشرة، فعلى سبيل المثال في بورصة "نيويورك" هبوط إحدى الشركات بهذه النسبة يعني تحمل خسائر تتراوح ما بين ٥٠ مليونا و٢٠٠ مليون دولار[٢٢].

وكما تؤدي الهجمات الإلكترونية إلى هز ثقة العملاء في الشركة، وهذا الأمر له أهمية كبيرة وخاصة بالنسبة للمؤسسات المالية، مثل المصارف وشركات التأمين التي تحتفظ ببيانات شخصية ومالية حساسة تخص عملائها، فإذا شاع خبر تعرضها للهجمات يفضل العملاء غالبا التحول إلى مؤسسة منافسة تتمتع بثقة أكبر في حماية سرية المعلومات.

وبالنسبة للجرائم الإلكترونية التي تتعرض لها كل من الشركات والبنوك يمكن ذكر ما يلي:

- الاطلاع على معلومات سرية بصفقة أو مناقصة أو غيرها من الأمور التسويقية.
- العبث بقواعد البيانات الخاصة بالشركة بحذفها أو تعديلها أو تعطيل الوصول إليها.
- سرقة الأموال وتحويل حسابات مصرفية خاصة بالشركة.
- الغش في المعاملات الإلكترونية.
- عمليات الاحتيال.
- التهديد والابتزاز.
- اختراق الموقع الإلكتروني الخاص بالشركة أو البنك.
- العبث بمخازن المعلومات الخاصة بالبنك بحذفها أو تعديلها أو تعطيل الوصول إليها.
- تعطيل النظام، ونقل ملكية الأسهم[٢٣].

٣. **أثر الهجمات الإلكترونية على الحكومات والدول:** من نتائج تقدم تقنيات الحاسب الآلي، ظهور الحكومة الإلكترونية، وظهور شبكات مرتبطة ببعضها البعض في داخل المصلحة أو المؤسسة الحكومية وفيما بعد تم ربطها بشبكة الإنترنت، وبهذا أصبح بمقدور الأفراد القيام بمصالحهم في نطاق الحكومة الإلكترونية[٢٤].

وبقدر ما حقق التقدم العلمي من رفاهية وتيسير لشؤون الأفراد والحكومات في انتهاج الحكومة الإلكترونية، بقدر ما زاد التهديد وزادت الهجمات الإلكترونية على الدول، حتى أن البعض من الدول تواجه حربا إلكترونية، وبالتالي زاد الخطر وزادت توجسات الدول من هذه الهجمات، ففي عهد الرئيس الأمريكي "بيل كلنتون" شكل لجنة خاصة مهمتها حماية البنية التحتية الحساسة في أمريكا[٢٥].

وفي هذا المجال صدر تقرير من وزارة الدفاع الأمريكية عام ١٩٩٧ يحذر من "بيرل هاربر إلكترونية"، وتوقعت أن تزداد الهجمات على نظم المعلومات في الولايات المتحدة الأمريكية، وأوضح التقرير أن شبكة الاتصالات ومصادر الطاقة الكهربائية والبنوك وصناعات النقل في أمريكا معرضة أكثر للهجوم من قبل أي جهة تسعى لمحاربة الولايات المتحدة الأمريكية(٢٦).

ومن الجرائم التي تتعرض لها الدول نذكر منها:

- الوصول إلى معلومات سرية والاطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم.
- دعم الإرهاب والأفكار المتطرفة ونشر الإشاعات.
- تعطيل وتخريب الخوادم الموفرة للمعلومات.
- تعطيل قطاعات حكومية حيوية في الدولة.
- تعطيل الإنترنت بالكامل.
- سرقة الأموال(٢٧).

المحور الثاني: استراتيجية مكافحة الجريمة المعلوماتية على الصعيد الدولي:

لقد أدرك المجتمع الدولي أن الجريمة المعلوماتية لم تعد مشكلة دولة ما، بل وصلت القناعة على المستوى الدولي إلى تكثيف الجهود على المستوى الدولي إلى ضرورة مكافحتها، خاصة بعد تزايد الخسائر الناجمة عن الحاسب الآلي، وتزايدت معها الخسائر المادية إذ بلغت حسب تقديرات بعض الخبراء إلى ١٢،٩٥٠ مليار دولار سنويا(٢٨)، ولم تقتصر الهجمات على المؤسسات المالية والحكومات بل تعدى الخطر ليمس كل فرد لديه بيانات إلكترونية قصد سرقتها أو ابتزازه بها، ومنه بات التعاون الدولي لمواجهة الجريمة المنظمة (الجريمة الإلكترونية) أمر حتمي، وفي هذا الإطار هناك العديد من المنظمات الدولية التي بذلت جهدا كبيرا في إبرام الاتفاقيات في محاولة منها لترسيخ وجوب التعاون الدولي لمواجهة جرائم الحاسب الآلي وعلى رأس هذه المنظمات نذكر كل من هيئة الأمم المتحدة والمجلس الأوروبي، وغيرها من المنظمات.

١. جهود الأمم المتحدة في مكافحة الجريمة المعلوماتية: لقد كرست الأمم المتحدة جهودها لمحاربة الجريمة المنظمة عبر الوطنية على اعتبار أنها تشكل تهديدا حقيقيا للسلم والأمن الدولي، وفي سنة ١٩٨٥ كلف مؤتمر الأمم المتحدة المنعقد "بميلانو" لجنة الخبراء العشرين بدراسة موضوع حماية نظم المعلومات وظاهرة الاعتداء على الحواسيب، وقد أقرت هذه المجموعة جملة من المقترحات والتوصيات، والتي تم تبينها في مؤتمر "هافانا" الكوبية في المؤتمر الثامن بعدما تم إدخال بعض التعديلات عليها، وتتمثل هذه التوصيات فيما يلي(٢٩):

- تحديث القوانين الجنائية الوطنية بما في ذلك التدابير المؤسسية.
- تحسين أمن الحاسب الآلي والتدابير المعينة.
- اعتماد إجراءات تدريب كافية الموظفين والوكالات المسئولة عن منع الجريمة الاقتصادية والجرائم المتعلقة بالحاسب الآلي والتحري والادعاء فيها.
- تلقين آداب الحاسب الآلي كجزء من مفردات مقررات الاتصالات والمعلومات .
- اعتماد سياسات تعالج المشكلات المتعلقة بالمجني عليهم في تلك الجرائم.
- زيادة التعاون الدولي من أجل مكافحة هذه الجرائم(٣٠).

وفي مؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاملة المجرمين الذي انعقد في القاهرة عام ١٩٩٥ أكد هذا المؤتمر في توصياته على ضرورة حماية الإنسان في حياته الخاصة وفي ملكيته الفردية من تزايد مخاطر التكنولوجيا، وضرورة وجوب التنسيق والتعاون الدولي قصد اتخاذ الإجراءات الكفيلة للحد منها.

وفي عام ٢٠٠٠ عقدت الأمم المتحدة مؤتمرها العاشر لمنع الجريمة ومعاملة المجرمين في بودابست المجرية، وقد أكد المؤتمر على وجوب العمل للحد من جرائم الحاسب الآلي المتزايدة والمستحدثة واتخاذ التدابير الكفيلة للحد من أعمال القرصنة(٣١).

٢. دور المنظمة العالمية للملكية الفكرية– wipo–: تعتبر هذه المنظمة إحدى الوكالات المتخصصة التابعة للأمم المتحدة اعتبارا من ١٧ ديسمبر ١٩٧٣، وقد بذلت هذه المنظمة جهدا معتبرا لحماية الملكية الفكرية، ومن أبرز النتائج التي وصلت إليها هذه المنظمة هو عدم اعتبار برامج الحاسب الآلي من قبل الاختراعات وخضوعها إلى حماية حق المؤلف، وتم التوصل إلى هذا بعدما شكلت

هذه المنظمة لجنة من الخبراء بهدف حماية برامج الحاسب الآلي، وقد تم تأكيد النتائج المتوصل إليها من طرف خبراء المنظمة في الاتفاقية الأوروبية لبراءة الاختراع التي تم توقيعها في "ميونخ الألمانية" في أكتوبر ١٩٧٣[٣٢].

ألا أن دور المنظمة العالمية للملكية الفكرية قد تقلص نوعا ما، في إطار اتفاقية التجارة العالمية الجات "GATT" لسنة ١٩٤٧، وعبر جولاتها التفاوضية الثمانية وصولا إلى جولة "الأروجواي" ١٩٩٤، والتي نتج عنها منظمة التجارة العالمية– WTO–، وقد عهد إليها مهمة تنفيذ اتفاقيات دورة "الأروجواي" التي تقع في ثلاث مجموعات أبرزها يتعلق بمواصفات التجارة المرتبطة بحقوق الملكية– تريبس TRIPS–[٣٣].

وفي عام ١٩٩٦ أبرمت اتفاقية بين منظمة التجارة العالمية والمنظمة العالمية للملكية الثقافية من أجل التعاون المشترك في مجال الملكية الفكرية لاسيما ما يتعلق منها بتطبيق بنود اتفاقية "تريبس".

٣. دور المجلس الأوروبي: لقد أقر المجلس الأوروبي مجموعة من القواعد التوجيهية في مجال الحماية من الجرائم المعلوماتية، ففي ١٩٨٠/٠٩/١٧ أقر المجلس الأوروبي والسوق الأوروبية المشتركة معاهدة مجلس أوروبا الخاصة بحماية الأشخاص من مخاطر المعالجة الآلية للبيانات، وقد دخلت هذه الاتفاقية حيز النفاذ في أكتوبر ١٩٨٥، وقد اقتصر تطبيق الاتفاقية على الأشخاص الطبيعيين في القطاع العام والخاص[٣٤].

ويظهر دور المجلس الأوروبي بشكل بارز بإصدار الاتفاقية المتعلقة بجرائم الحاسب في ٢٠٠٠/٠٤/٢٥، وذلك في اجتماع المجلس في "ستراسبورغ الفرنسية"، وجاءت هذه الاتفاقية لتؤكد حرص الدول الأعضاء على حماية مجتمعاتها من جرائم الحاسب الآلي، وضرورة وضع التشريعات الملائمة وتعزيز التعاون الدولي سيما مع تزايد الاعتداء على المعلومات الإلكترونية[٣٥].

كما أصدر الاتحاد الأوروبي العديد من التوجيهات لحماية قواعد البيانات بوصفها نتاجا فكريا، فبتاريخ٠٣،١١، ١٩٩٦ صدرت التوجيهة رقم (CEE/٩/٩٦) تتعلق بالحماية القانونية لقواعد البيانات بما في ذلك غير الإلكترونية، كما صدر عن الاتحاد الأوروبي توجيه آخر سنة ١٩٩٩ يتجه نحو مناغمة بعض مظاهر حق المؤلف والحقوق المجاورة في مجتمع المعلومات، وتضمنت المادة الخامسة من التوجيهة الأوروبية على: ....السماح بالنسخ العابر والقانوني... عندما يكون الغاية الوحيدة منه استخدام العمل من دون أن يكون للنسخ في هذه الحالة أي مدلول اقتصادي مستقل..."[٣٦].

وفي الأخير، وبالنسبة لحقوق المؤلف على شبكة الإنترنت صدرت بعض النصوص المنظمة لذلك في اتفاقية "تريبس" ثم تلاها التنظيم الوارد في معاهدتا "الويبو

" اللتان عرفتا باسم معاهدتا الإنترنيت والصادرتان عام ١٩٩٦ تحت اسم معاهدة "الويبو" بشأن حق المؤلف، ومعاهدة "الويبو" بشأن الأداء والتسجيل الصوتي، وذلك لأن النسخ الإلكتروني دون إذن أو ترخيص يعد اعتداء على حق المؤلف والحقوق المجاورة[٣٧].

المحور الثالث: **استراتيجية مكافحة الجريمة المعلوماتية على الصعيد العربي**:

تعد التشريعات العربية متأخرة في مواكبة المستجدات التشريعية العالمية المتعلقة بجرائم الحاسب الآلي رغم أن خطر الجرائم المعلوماتية والإنترنت على البيئة العربية يكاد يكون أخطر وأكبر لكون عدم الجاهزية الأدائية والتقنية والتشريعية، ووضع الاستراتيجيات لحماية ومواجهة الحرب الإلكترونية ليست في المستوى المطلوب في بعض الدول، إن لم تكن في البعض الآخر[٣٨].

ولكن هذا لا يعني عدم وجود جهود قصد مواجهة الجرائم الإلكترونية على المستوى العربي، فيعتبر القانون الجزائي العربي الموحد المعتمد من طرف مجلس وزراء العدل العرب، بموجب القرار رقم ٢٢٩ لسنة ١٩٩٦ أحد أهم المبادرات العربية في سبيل مكافحة الجريمة المعلوماتية[٣٩].

١. القانون الجزائي العربي الموحد: لقد تضمن القانون الجزائي العربي الموحد في الباب السابع الخاص بالجرائم ضد الأشخاص، فصلا نظم أحكام الاعتداء على حقوق الأشخاص الناتج الجذاذات[٤٠] والمعالجات المعلوماتية وذلك بموجب المواد ٤٦١– ٤٦٤، كما تضمنت المواد ٤٦١– ٤٦٣ وجوب حماية الحياة الخاصة وأسرار الأفراد من خطر المعالجة الآلية، وكيفية جمع المعلومات الاسمية وكيفية الاطلاع عليها وأما المادة ٤٦٤ فقد نصت على توقيع العقاب على كل من يقوم بفعل الدخول بطريق الغش إلى كامل أو جزء من نظام المعالجة الآلية للمعلومات، وعرقلة أو إفساد نظام التشغيل عن أداء وظائفه المعتادة وتغيير المعلومات داخل النظام، وتزوير وثائق المعالجة الآلية وسرقة المعلومات[٤١].

ونشير أن هذه المحاولات العربية تعتبر محتشمة بالمقارنة مع حجم الهجمات الإلكترونية، التي ارتقت إلى درجة الحرب الإلكترونية، وبالتالي من غير المقبول أن تواجه هذه الحرب بهذه اللامبالاة، حتى ولو أن بعض الدول تسعى إلى وضع منظومة قانونية وفنية لمواجهة هذه الظاهرة، إلا أنها لن تكون بالقدر الفعال إذا لم تدعم بالتعاون الدولي سواء على الصعيد الإقليمي العربي، أو على الصعيد الدولي.

وأما فيما يخص حماية الملكية الفكرية فقد تم إبرام الاتفاقية العربية لحماية حقوق المؤلف من طرف الوزراء العرب المسئولين عن الثقافة سنة ١٩٩١ ببغداد، كما أبرمت المنظمة العربية للتربية والثقافة والفنون الاتفاقية العربية لتيسير انتقال الإنتاج الثقافي العربي في عام ١٩٨٧[٤٢].

وتعتبر هذه الاتفاقيات جهدا متواضعا من طرف المنظمات التابعة للجامعة العربية في إطار تنظيم حقوق المؤلف من جرائم الحاسوب، إلا أن تفعيل هذه الاتفاقيات في أرض الواقع لا يكاد يلاحظ ويلمس ولعل هذا يرجع إلى تواضع الإنتاجات الفكرية الرقمية في الوطن العربي، وبالتالي فإن أثر الجرائم الماسة بالملكية الفكرية في الوطن العربي هي أقل بكثير منها في الدول الغربية.

٢. الجهود العربية الفردية لمواجهة الجريمة المعلوماتية: لا يمكن الحديث عن مواجهة الجريمة المعلوماتية دون الحديث عن جهود بعض المنظمات ومراكز البحث المتخصصة والجامعات، وما تلعبه من دور لا يستهان به في مجال مكافحة الجريمة الإلكترونية، ونشير في هذا الصدد على سبيل المثال لا الحصر ما تقوم به الجمعية المصرية للقانون الجنائي، فقد عقدت مؤتمرها السادس في أكتوبر من عام ١٩٩٣ بالقاهرة حول جرائم الكمبيوتر والجرائم الأخرى في مجال تكنولوجيا المعلومات، حيث أكد فيه المؤتمرون بأن الجرائم المعلوماتية أصبحت جرائم عالمية تتخطى الأوطان، كما دعوا إلى ضرورة تكاثف الجهود لمحاربتها، وكذلك وجوب تعديل نصوص قوانين العقوبات التقليدية، كما خرج المؤتمرون بتوصيات خاصة بأنماط وطوائف جرائم الحاسب الآلي، وبالتعاون الدولي في مجال أنظمة المعلومات وبوجوب تدريب رجال الضبطية القضائية والنيابة العامة والقضاة على طرق وكيفية استخدام أجهزة المعلومات وطرق التحري والاستدلال فيها[٤٣].

وتم في العاصمة الأردنية عمان عقد المؤتمر الدولي الأول للملكية الفكرية عام ١٩٩٥، وناقش المؤتمرون حماية الملكية الفكرية والإجراءات المطلوبة من طرف الدول العربية لتنفيذ اتفاقية- تريبس- وأثر حماية الملكية الفكرية على مستقبل الاستثمارات في منطقة الشرق الأوسط[٤٤].

كما خرج المؤتمر الذي عقد ببيروت عام ١٩٩٧ بتوصيات تمثلت في ضرورة إنشاء محاكم متخصصة للبث في النزاعات المتعلقة بالحماية وتشجيع التعاون بين الدول العربية، وأما المؤتمر العربي الثاني للملكية الفكرية المنعقد عام ١٩٩٨، أوصى بضرورة تسهيل نقل التكنولوجيا من الدول الصناعية إلى الدول العربية لحماية الاختراعات ومكافحة القرصنة وتسهيل نقل اختراعات العلماء العرب إلى أوطانهم[٤٥].

خاتمة:

وفي خاتمة هذه المداخلة نشير إلى مقولة قاضي فرنسي حول المعلومة بقوله: "إن المعلومة قوة اقتصادية والقدرة على تخزين أنواع معينة من البيانات ومعالجتها يمكن أن يعطي بلدا مميزات أساسية وتكنولوجية على البلدان الأخرى، وهو ما قد يؤدي إلى فقدان السيادة الوطنية لتلك البلدان من خلال انتقال تلك البيانات فيما بين الدول"، ويكفينا مثلا في هذا المقام الإشارة إلى الولايات المتحدة الأمريكية وهي أقوى دولة من الناحية المعلوماتية وكيف وقعت ضحية للتطور الذي وصلت إليه، وذلك من خلال تسريب المعلومات من طرف شخص يدعى "سندون" ومدى الضرر الذي لحق بالولايات المتحدة الأمريكية.

وعليه قد أصبحت الجريمة المعلوماتية جريمة لا تهدد دولة بعينها، وإنما تجاوزت حدود الدولة الواحدة، وأصبحت جريمة عابرة الحدود، وإن كان بعض الدول قامت بوضع منظومة قانونية لمواجهة هذه النوع الجديد من الإجرام، ونشير أن أول بلد سن قوانين خاصة بجرائم الحاسب الآلي هو السويد عام ١٩٧٣، ثم تلى ذلك كل من الولايات المتحدة الأمريكية، وبريطانيا وكندا وغيرها من الدول الغربية وأما بالنسبة للدول العربية فتعتبر الإمارات العربية المتحدة دولة رائدة في مجال مكافحة الجرائم المعلوماتية وكذلك المملكة العربية السعودية وتونس ومصر ولبنان، وبالنسبة للجزائر فقد سن المشرع الجزائري القانون رقم ٠٩-٠٤ المؤرخ في ١٤ شعبان ١٤٣٠ الموافق لـ٠٥ أوت ٢٠٠٩ المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها.

وفي ختام هذه المداخلة نصل إلى اقتراح التوصيات التالية:

- ضرورة نشر ثقافة المعلومات على المستوى الفردي، وتوعية الأفراد من المخاطر التي تتهددهم فمن غير المقبول أن يتلقى الفرد على سبيل المثال رسالة إلكترونية تخبره بأنه الفائز بورقة اليانصيب ويجب عليه التعجيل بإرسال بياناته الشخصية أو مبلغ مالي معين ليحصل على المبلغ، على الرغم من أنه لم يشارك قط في اليانصيب، فالمؤمن كيس فطن، ولا يلدغ المؤمن من الجحر مرتين.
- وجوب تدريب العاملين الحكوميين وتوعيتهم، وبخاصة الذين يشتغلون بمناصب حيوية، فلا يعقل أن يستعمل الفرد الحاسب الآلي للحكومة لأغراضه الشخصية وتحميل البرامج وغيرها، وذلك لما ينطوي عليه الأمر من خطورة الاختراق أو إصابة الخوادم أو الحاسب الآلي بالفيروسات.
- وضع خطة وطنية استراتيجية لمكافحة الجريمة المعلوماتية، ودراسة احتمالات الهجمات الإلكترونية وضع خطة طوارئ أو الخطط البديلة في حالة الهجمات الإلكترونية.
- تأهيل الفنيين ومنفذي القانون من شرطة وقضاة وتمكينهم من المعارف الجديدة قصد أداء وظائفهم وإمكانية تعاملهم مع الجرائم الحديثة.
- تفعيل دور الشرطة العربية وتزويدها بالوسائل القانونية والفنية قصد تعقب الجرائم الإلكترونية والمجرمين في الوطن العربي، والتنسيق مع الأجهزة الأخرى "كالأنتربول"، و"اليوروبول" وغيرها من المنظمات التي تعني بمكافحة الجريمة عبر الوطنية.
- ضرورة التعاون بين الدول سواء على المستوى الإقليمي العربي أو على المستوى الدولي، فالجريمة المعلوماتية لا يمكن أن تواجها دولة لوحدها، بل لابد من تكثيف الجهود بين الدول سواء من خلال التنسيق الأمني والقضائي، وكذلك تبادل المعلومات والخبرات لمواجهة الجريمة المعلوماتية.

المراجع:

[١] د. علي جبار الحيسناوي، جرائم الحاسوب والإنترنت، دار اليازوردي العلمية للنشر والتوزيع، طبعة ٢٠٠٩، ص١٨.

[٢] يونس عرب، موسوعة القانون وتقنية المعلومات، دليل أمن المعلومات والخصوصية- جرائم الكمبيوتر والإنترنت، منشورات اتحاد المصارف العربية، الجزء الأول، الطبعة الأولى ٢٠٠٢، ص٢، ٣.

[٣] من أمثلة الجرائم التي تضمنتها الدراسة يمكن ذكر، جريمة استخدام ونشر الشفرة الخبيثة ، جريمة استخدام غير مصرح به للحواسيب، جريمة هجمات حجب الخدمة، جريمة تدمير البيانات الحاسوبية، جريمة سرقة وتعديل البيانات، جريمة انتهاكات البريد الإلكتروني، جريمة انتحال الهوية الحاسوبية، وغيرها من الجرائم الإلكترونية التي لا يسع المجال لذكرها جميعا.

[٤] محمد أمين الشوابكة، جرائم الحاسوب والإنترنت، الجريمة المعلوماتية، دار الثقافة عمان- الأردن- الطبعة الأولى ٢٠٠٤، ص٧٤.

[٥] دياب موسى البداينة، الجرائم الإلكترونية: المفهوم والأسباب، ورقة علمية قدمت في الملتقى العلمي الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية والدولية، ٢-٤/٠٩/٢٠١٤، عمان المملكة الأردنية.

[٦] د. عبد الفتاح بيومي حجازي، الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتاب القانونية، جمهورية مصر العربية، طبعة ٢٠٠٢، ص٦.

[٧] نفس المرجع.

[٨] منى شاكر فراج العسبلي، تأثير الجريمة الإلكترونية على النواحي الاقتصادية، مقال منشور على الموقع الإلكتروني لمركز التميز للأمن المعلوماتي، www.coeia.edu.sa

[٩] نفس المرجع.

[١٠] محمد أمين الشوابكة، المرجع السابق، ص١٧٩.

[١١] منى شاكر فراج العسبلي، المرجع السابق.

[١٢] نفس المرجع.

[١٣] السنتيمات هي أجزاء من الوحدة النقدية، فيقال دينار وعشرون سنتيما، أي عشرون جزءا من الدينار.

[١٤] نديم عبده، أمن المعلومات، مجلة الكمبيوتر والاتصالات والإلكترونيات، المجلد ١٧ العدد السادس، أوت ٢٠٠٠ ص٤٠.

[١٥] محمد أمين الشوابكة، المرجع السابق، ص٢٠٠-٢٠٠١.

[١٦] المرجع نفسه.

[١٧] منى شاكر فراج العسبلي، المرجع السابق.
[١٨] نفس المرجع.
[١٩] محمود أحمد عبابنة، جرائم الحاسوب وأبعادها الدولية، دار الثقافة، عمان، ٢٠٠٥، الطبعة الأولى، ص١٥٢.
[٢٠] سامي علي حامد عياد، الجريمة المعلوماتية وإجرام الإنترنت، دار الفكر الجامعي، الإسكندرية، طبعة ٢٠٠٧، ص٧٢.
[٢١] نفس المرجع.
[٢٢] د. علي جبار الحيسناوي، المرجع السابق، ص١٤٨.
[٢٣] نفس المرجع.
[٢٤] د. عبد الفتاح بيومي حجازي، النظام القانوني لحماية الحكومة الإلكترونية، دار الفكر الجامعي، الطبعة الأولى ٢٠٠٣ ص١٧٢.
[٢٥] سامي علي حامد عياد، المرجع السابق، ص٩٢.
[٢٦] نفس المرجع.
[٢٧] منى شاكر فراج العسبلي، المرجع السابق.
[٢٨] معلومات مستقاة من الموقع الإلكتروني: http://www.aldaawah.com/?p=٧٨٣٣
[٢٩] منى شاكر فرج العسبلي، المرجع السابق.
[٣٠] مقال عبد اللاله مجيد منشور على الموقع الإلكتروني: http://www.elaph.com/Web/News/٢٠١٤/٦/٩١٢٤٨٥.html
[٣١] منى شاكر فراج العسبلي، المرجع السابق.
[٣٢] د. إبراهيم أحمد إبراهيم، الحماية القانونية لبرامج الكمبيوتر، بحث منشور في مجلة التحكيم والقانون، جانفي ١٩٩٧ ص٧٣.
[٣٣] فتحت الاتفاقية للدول الأعضاء فترة انتقالية للتوافق مع أحكام تريبس، انتهت بالنسبة للدول النامية في العام ٢٠٠٠، وتنتهي للدول أقل نموا في العام ٢٠٠٦.
[٣٤] د. محمد فتحي عيد، الإجرام المعاصر، أكاديمية نايف العربية للعلوم الأمنية، الرياض، الطبعة الأولى، ١٩٩٩، ص٢٥٥.
[٣٥] د. علي جبار الحيسناوي، المرجع السابق، ص١٥١، د. محمود أحمد عبابنة، المرجع السابق، ص ١٦٥.
[٣٦] وليد الزيدي، القرصنة على الإنترنت والحاسوب، التشريعات القانونية، دار أسامة، عمان الأردن، الطبعة الثانية، ٢٠٠٣، ص١٢٥.
[٣٧] نفس المرجع.
[٣٨] محمود أحمد عبابنة، المرجع السابق، ص١٧١.
[٣٩] نفس المرجع.
[٤٠] الجذاذ في معجم المعاني الجامع والمعجم البسيط، الجذاذ المقطع أو المكسر، وجذاذة معلومات، وريقات صغيرة تقيد بها المعلومات للاحتفاظ بها لمراجعتها.
[٤١] اعتمد مجلس وزراء العدل العرب القانون الجزائي العربي الموحد كقانون نموذجي بالقرار رقم ٢٢٩- د١٢- المؤرخ في ١٩٩٦/١١/١٩، وللتفصيل أكثر والاضطلاع على القانون راجع الموقع الإلكتروني التالي: www.carjj.org
[٤٢] توصيات المؤتمر السادس للجمعية المصرية للقانون الجنائي المنعقد بالقاهرة من الفترة الممتدة ما بين ٢٥-٢٨ أكتوبر ١٩٩٣.
[٤٣] د. علي جبار الحيسناوي، المرجع السابق، ص١٦١.
[٤٤] المؤتمر العربي الأول للملكية الفكرية، الأردن- عمان-، ٢٨-٣٠ سبتمبر ١٩٩٥، تنظيم مشترك بين المجمع العربي لحماية الملكية الصناعية، أبو غزالة للملكية الفكرية تي. أم. بي. أجتتس.
[٤٥] نفس المرجع.